National Infrastructure Protection Center CyberNotes

Issue #3-99 *February 3 , 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between January 16 and January 27, 1999. The table provides the operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site. Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Cisco IOS[1]	Operating System	Any Cisco device running IOS code will identify the fact that it is a Cisco product when a SYN packet is sent to port 1999.	Workaround is to deny incoming Transmission Control Protocol (TCP) connections to port 1999 where possible.	Remote Cisco Identification	Low/ Medium	Bug discussed in newgroups. Exploit script posted to newsgroups and Web sites.
Linux[2] 2.0.36	Operating System	Local user can cause a Denial-of-Service (DoS) on ports above 1024.	Versions 2.1.X and 2.2.X-prebuild are not affected.	2.0.36 local user DoS	Low	Exploit script posted to newsgroups and Web sites.

[1] BUGTRAQ, January 18, 1999.
[2] BUGTRAQ, January 19, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Linux[3] (may also affect FreeBSD prior to Perl 5 implementation)	Operating system and Perl	It is possible for an unauthorized local user to gain root access using a setuid Perl script on a CD-ROM or floppy disk.	No workarounds or patches known at time of publishing.	Linux suidperl	Medium/ High	Bug discussed in newgroups.
Linux[4] – Debian GNU 1.3	FTPwatch	Unauthorized users can gain root access.	Authors recommend removing FTPwatch immediately.	Debian Linux FTPwatch	High	Bug discussed in newgroups.
Microsoft[5]	Internet Explorer 4 (IE4)	IE4, under certain circumstances, fails to close connections to a proxy server. This can open the session to man-in-the-middle attacks/spoofs.	No workarounds or patches known at time of publishing.	IE4 Persistent Keepalive Bug	Low	Condition discussed in newsgroups.
Microsoft[6]	Applications using Forms 2.0 ActiveX control (any application that includes Visual Basic for Applications 5.0)	Unauthorized Web site or maliciously constructed HyperText Markup Language (HTML) email can reveal items contained in the clipboard.	Patch is available at: http://support.microsoft.com/support/kb/articles/q214/7/57.asp	Forms 2.0 ActiveX Clipboard	Low	Bug discussed in newgroups. Exploit script posted to newsgroups and Web sites.
Microsoft Windows[7]	Internet Information Server 4 (IIS 4) with sample site ExAir loaded	Direct request to three of the ExAir files will cause a DoS condition for 90 seconds even if ExAir was not loaded.	Workaround is to remove: ExAir – root/search/advsearch.asp, ExAir – root/search/query.asp, and ExAir – root/search/search.asp	ExAir sample site DoS	Low	Bug discussed in newgroups and Web sites. Exploit script is not required for the exploit.
Microsoft Windows[8]	IIS	If upgrading from IIS 2 or 3 to 4, a dll called ism.dll is left in /scripts/iisadmin. An unauthorized user can gain access to sensitive server information, including potentially the Administrator's password.	Remove ism.dll from /scripts/issadmin.	IIS upgrade ism.dll	Medium	Bug discussed in newgroups and Web sites. Exploit script not required for the exploit.
Microsoft Windows[9]	IIS	IIS will not log requests if the path is over approximately 10,100 bytes. The request will still be honored.	Workaround is to use additional logging methods.	IIS long path request	Low	Bug discussed in newgroups and Web sites. Exploit script not required for the exploit.

[3] BUGTRAQ, January 14, 1999.
[4] Debian security announcement, January 17, 1999.
[5] BUGTRAQ, January 22, 1999.
[6] Microsoft Security Bulletin, MS99-001
[7] NTBUGTRAQ, January 26, 1999.
[8] BUGTRAQ, January 14, 1999.
[9] Provider requested anonymity.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows[10]	IIS and perl.exe	On all versions of ISS, a request for a non-existent file will return the physical location of the Web directory on the machine.	Workaround is to use the perlis.dll instead of perl.exe. You can use perl.exe and have IIS check for the file's existence.	perl.exe and IIS	Low	Bug discussed in newgroups and Web sites.
Microsoft Windows[11] 95, 98, and NT[12]	IIS and File Transfer Protocol (FTP)	Unauthorized remote user can log in (anonymous access included) and create a DoS condition. This may be a result of a stack overflow or bss (static pointers) overflow.	Specific configurations appear to be necessary for the vulnerability to occur. NT + Option pack 4 + SP 4 or NT + IIS3 + SP 4 or PWS 1.0 No workarounds or patches known at time of publishing.	IIS DoS FTP	Low/ Medium	Script identified at time of publishing but does not appear to be posted. Explanation of exploit available in newsgroups.
Microsoft Windows[13] NT	IIS (installed from NT Option Pack and FrontPage Server Extensions)	A buffer overflow that exists in the program that may allow unauthorized users to execute commands.	Obtain FrontPage Server Extensions 98 from: http://www.microsoft.com/frontpage.	IIS on NT with FrontPage buffer overflow	Medium/ High	Bug discussed in newgroups and Web sites. References to exploit script found.
Microsoft Windows[14] NT	Quakenbush Windows NT Password Appraiser	When Internet Query option is selected, the standard and professional versions send LANMAN hashes and the decoded password in the clear across the Internet.	Update issued to the Password Appraiser program (standard and professional).	Quakenbush password problem	Medium/ High	Default condition discussed in newsgroups. Hacker tools exist that can decrypt password hashes.
Multiple[15]	Computer Associates' (CA) ControlIT enterprise management software	Use of weak password encryption when transmitting passwords over the Internet could enable a hacker to obtain user and administrator passwords on Microsoft Windows NT machines.	CA recommends using ControlIT's "built-in" security, because NT usernames/passwords are not required.	ControlIT weak password encryption	Medium/ High	Bug discussed in newgroups. Hackers typically install sniffers on networks. Sniffers will capture the NT username/ password if used.
Multiple[16]	CA's ControlIT enterprise management software	When "reboot on disconnect" is enabled, any invalid username/password will reboot the system.	CA has a patch available at http://www.cai.com or by calling 1-800-DIALCAI.	ControlIT reboot on invalid username/ password	Medium (High - if you have machine that performs critical functions)	Bug discussed in newgroups and Web sites. Exploit script not required for the exploit.

[10] NTBUGTRAG, January 26, 1999.
[11] eEye Digitial Security Team, Advisory Code - IISE01.
[12] BUGTRAQ, January 25, 1999.
[13] BUGTRAQ, January 14, 1999.
[14] L0pht Security Advisory, January 21, 1999.
[15] IIS Security Advisory, Multiple vulnerabilities in ControlIT.
[16] Ibid.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple[17]	BackWeb Technologies' BackWeb Polite Agent Protocol	Unauthorized individual may be able to hijack sessions between client and server. This hijacking could result in the delivery of unwanted software.	Upgrade to V5.0.	BackWeb Polite Agent Spoofing	Low/ Medium	Bug discussed in newgroups and Web sites. Exploit script not required for the exploit.
Multiple[18]	DPEC Online Courseware	Unauthorized user can gain access to and change the password of any user, including admin.	No workarounds or patches known at time of publishing.	DPEC Online Courseware password problem	Low	Bug discussed in newgroups and Web sites.
Multiple[19]	Lotus Notes (Windows and Sun Solaris versions)	Multiple long strings (2,048 characters) establishing connections (helo A and then helo B) cause a DoS condition.	No workarounds or patches known at time of publishing.	Lotus Notes long string DoS	Low	Bug discussed in newgroups.
Multiple[20]	Most Web servers	It is possible to confuse Hypertext Transfer Protocol (HTTP) logging with the use of special characters in REQUEST_METHOD.	Workaround is to use additional logging methods.	HTTP REQUEST_ METHOD flaw	Low	Bug discussed in newgroups and Web sites.
Multiple[21]	Multiactive's Maximizer	Unauthorized individual has the ability to alter data.	No workarounds or patches known at time of publishing.	Maximizer data change	Low	Bug discussed in newgroups and Web sites.
Multiple[22]	Sscan (0.1 alpha)	Unauthorized user can execute buffer overflow conditions.	Update to new version (See "Recent Exploit Scripts" below for explanation).	sscan	Low	Default condition discussed in newsgroups.
Sun Solaris[23] 2.6	Operating System	On some installations using Network Information Services (NIS) and NIS+, an unauthorized individual can directly connect without using portmapper. This connection will provide hashed passwords.	Workaround is to use /var/yp/securenets, which provides a secure distributed name service. Further details are available at: http://www.sunworld.com/sunworldonline/common/security-faq.html.	NIS and NIS+ ephemeral ports	Medium/ High	Bug discussed in newgroups and Web sites. Hackers known to be attempting to exploit.

[17] ISS Security Advisory, Vulnerability in the BackWeb Polite Agent Protocol.
[18] BUGTRAQ, January 15, 1999.
[19] BUGTRAQ, January 15, 1999.
[20] BUGTRAQ, January 6, 1999.
[21] BUGTRAQ, January 14, 1999.
[22] BUGTRAQ, January 20, 1999.
[23] BUGTRAQ, January 13, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Sun Solaris[24] 2.5.1 (unpatched)	Operating System	Any process that runs with a user's privilege is susceptible to tracing by the user.	Patch for version 2.5.1 is kernel update 103640.	Solaris 2.5.1 user tracing problem	Low/ Medium	Bug discussed in newgroups.
Unix[25]	TCP Wrappers 7.6	A Trojan horse version of the program (tcp_wrappers_7.6.tar.gz) was placed on numerous sites. Unauthorized user can gain root access.	Obtain new version of TCP Wrappers if you downloaded the program since January 20, 1999. Workaround is to block port 421 source, not destination, if possible.	TCP Wrappers Trojan horse (Note: some sources have called this the Unix version of Back Orifice)	High	Hackers known to be attempting to exploit this Trojan horse.
Unix – Digital[26] 4.0 prior to 4.0D	Operating System (at)	Buffer overflow condition exists in "at" that can allow an unauthorized user to gain root access.	Upgrade to Digital Unix 4.0D or obtain appropriate patch from: ftp://ftp.service.digital.com/public/dunix.	Digital Unix at buffer overflow	High	Script identified at time of publishing but does not appear to be posted. Explanation of exploit available in newsgroups.
Unix – Digital[27] 4.0	Operating System (inc)	Buffer overflow condition exists in /usr/bin/mh/inc that can allow an unauthorized user to gain root access.	No workarounds or patches known at time of publishing.	Digital Unix inc buffer overflow	High	Script identified at time of publishing but does not appear to be posted. Explanation of exploit available in newsgroups.
Unix[28] – NetBSD	Operating System	Unauthorized user may cause a DoS condition in TCP services due to select(2)/accept(2) race condition.	Patch available at: ftp://ftp.NetBSD.ORG under /pub/NetBSD/misc/security/patches/19990120-accept.	Net BSD Select (2)/Accept (2) race condition in TCP servers	Medium/ High	Exploit script (nmap) posted to newsgroups and Web sites. Hackers known to be using nmap with increased frequency.
Sun Solaris[29] 2.6, 2.6x86, 2.7, and 2.7x86	Operating System	Buffer overflow condition exists in /usr/bin/lpstat that can allow an unauthorized user to gain root access.	Workaround it to: chmod –s /usr/bin/lpstat chmod –s /usr/bin/lpq	Buffer overflow in Solaris /usr/bin/lpstat	High	Bug discussed in newgroups and Web sites. Hackers known to be attempting to exploit.
WEBRAMP[30]	Operating System	Default password allows full access to device.	Change default admin password.	WEBRAMP default admin password	High	Bug discussed in newgroups. Hackers known to be attempting to exploit.

[24] BUGTRAQ, January 13, 1999.
[25] CERT advisory CA-99-01-Trojan-TCP-Wrappers, revised January 22, 1999.
[26] BUGTRAQ, January 25, 1999.
[27] BUGTRAQ, January 25, 1999.
[28] BUGTRAQ, January 20, 1999.
[29] HERT advisory #001.
[30] BUGTRAQ, January 21, 1999.

Note: If you have recently purchased a CD-ROM, it is possible that patches released several weeks before your purchase are not included on the CD-ROM. CD-ROMs generally have cut-off dates for software additions weeks before they are available for purchase.

*Risk is defined in the following manner:

High – A vulnerability that will allow an intruder to immediately gain privileged access (e.g., Sysadmin, root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium – Any vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between January 16 and January 27, 1999, listed by date of script, script name, script description, and comments. Items listed in boldface (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches. Those items in red represent scripts that hackers/crackers are utilizing. During this time period, 48 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
Jan 27, 1999	Bandwidthrape	Explanation and sample exploit code that causes a remote server to consume large amounts of bandwidth.	
Jan 27, 1999	Cisco.c	Code segment that identifies Cisco equipment. See Remote Cisco Identification in "Bug, Holes & Patches" above.	
Jan 27, 1999	Digital-Unix4.0-asm-shell	Exploit code that uses a buffer overflow, which results in a root shell. This is a local exploit.	
Jan 27, 1999	Lpstat x86.c	Exploit code for the lpstat vulnerability in Sun Solaris 2.6/2.7 x.86.	
Jan 27, 1999	Spoof.c	Demonstration code for creating spoofed packets on Linux.	
Jan 27, 1999	Warp Scanner 2	Windows-based TCP port scanner.	
Jan 26, 1999	Apc.c	Unix password cracker.	
Jan 26, 1999	CGIchk2.c	Program that checks for Common Gateway Interface (CGI) vulnerabilities and, if any are found, will attempt to exploit the most common.	
Jan 26, 1999	Exploit Scanner v2.0	Scans subnet for many well-known Trojan horses and exploits.	
Jan 26, 1999	Mailwatch.c	Program that watches a user mailbox and notifies another user when mail is received.	
Jan 26, 1999	Ppscan.c	Program that allows the use of a proxy server to hide scan attempts when checking for Web servers.	
Jan 26, 1999	Ps.s	Script that bind a shell to port 46256.	
Jan 25, 1999	Cgiscan.c	Scanner that checks for various common vulnerabilities in CGI scripts.	
Jan 25, 1999	Manipulate_data v1.0	Code that allows the user to search a hard drive for data and then write it back after modification.	
Jan 25, 1999	Net-RawIP v0.04	Perl module that manipulates raw Internet Protocol (IP) packets and Ethernet headers.	
Jan 25, 1999	Oshare_1_gou.c	Exploit code the cause a DoS condition on Microsoft Windows 98 machines by issuing malformed packets.	
Jan 25, 1999	Page.sh	Unix shell script that checks for the FrontPage_vti_pvt/service.pwd exploit.	
Jan 25, 1999	RiP FTP server v1.0	Win32 program that captures File Transfer Protocol (FTP) passwords from server client software.	
Jan 24, 1999	Balu.pl	Program that exploits a vulnerability in mIRC 5.5's new dcc server feature. Places program in any destination directory on the same hard drive in which mIRC resides.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
Jan 24, 1999	Tgk-log v2.3	Recoded version of linsniffer that is designed to record contents of packets as they pass through an ipmasq gateway.	
Jan 24, 1999	UTIL-Linux-29g	Trojan horse version of util-Linux2.9g.	
Jan 24, 1999	Wsftp-hit	Exploit for ws-ftp design weakness that allows hackers to gain access to cached passwords.	
Jan 23, 1999	Icmpmon.c	Program that shows all ICMP packets received by the machine on which the program is running.	
Jan 23, 1999	M3-entre	Explanation of how to conduct attacks on the WEBRAMP default admin password and the default login/password. This script includes a text file with several suggestions on malicious uses. See "Bugs, Holes & Patches" section above.	
Jan 23, 1999	NetGuard v0.0.2	Combination of two programs that intercept and log TCP/IP and User Datagram Protocol (UDP)/IP connections. Allows limited logging of the TCP connections to syslog.	
Jan 22, 1999	ftp-spoof.pl	Program and instructions for altering site name of an FTP server, allowing any user to spoof its address.	
Jan 22, 1999	L0phtCrack 2.52 for Win95/NT	Password cracker for Microsoft Windows 95/NT. Improvements include 450% increase in speed, combination dictionary and numeric/symbol passwords.	
Jan 22, 1999	PoP-spoof.pl	Allows user to spoof a Post office Protocol (PoP) server and obtain passwords as clear text.	
Jan 22, 1999	TellME v0.1	Retrieves NetBIOS name from remote Microsoft Windows machines.	
Jan 21, 1999	Avoid	Program that tests for the IIS long path request.	
Jan 21, 1999	M3	Explanation of the WEBRAMP default admin password vulnerability. See "Bugs, Holes & Patches" section above.	
Jan 21, 1999	Quake2-bof-DOS	Explanation and exploit code for Quake2 buffer overflow DoS attack.	
Jan 20, 1999	Backwork v2.0	Trojan horse cleaner that states it is capable of identifying and removing 45 different Trojan horses.	
Jan 20, 1999	CGIc_DoS	Explanation and sample exploit code for a buffer overflow in the CGIc Library.	
Jan 20, 1999	Killport.c	Exploit code for the Linux local port/memory DoS attack. See Linux 2.0.36 local user DoS in "Bugs, Holes & Patches" section above.	
Jan 20, 1999	Resetter.c V2.1	DoS tool that attempts to reset all connections of a network segment by sending spoofed RST and ICMP UNREACHABLE packets.	
Jan 19, 1999	Against.c	Exploit code for the Sendmail 8.9.2 DoS problem.	
Jan 19, 1999	Backweb-spoof	Explanation of how to conduct an attack on BackWeb. See BackWeb Polite Agent Spoofing in "Bugs, Holes & Patches" section above.	
Jan 19, 1999	BusJack v1.0	Program that identifies and cleans the NetBus Trojan horse program.	
Jan 19, 1999	CISCO-IOS-ID	Code to automatically identify CISCO equipment. See Remote Cisco Identification in "Bugs, Holes & Patches" section above.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
Jan 19, 1999	Directory Snoop V2.1	Program that allows low-level review of disk drives on Microsoft Windows 95/98 machines.	
Jan 19, 1999	NetBus v2.0 Pro Beta	Trojan horse program with an improved Graphical User Interface (GUI), proxy support, file manager, web-cam capture, registry manager, hosts scheduler, and chat features.	
Jan 19, 1999	Net-RawIP v0.03	Perl module that manipulates raw IP packets and Ethernet headers.	
Jan 19, 1999	**Sscan v0.1 alpha**	**Improved version of mscan that is now configurable by "anyone with no programming knowledge."**	
Jan 19, 1999	TellMe v0.1	See explanation above.	
Jan 19, 1999	Vnmap	Tcl/Tk/wish-based front-end for nmap.	
Jan 19, 1999	Wyjeb.c	Local DoS that uses syslogd for the attack.	
Jan 19, 1999	xcrack	Unix/Linux Password cracking program written in Perl.	

Note: In the last edition of CyberNotes, in the "Recent Exploit Scripts" section under the name Gammaprog 1.4, the acronym POP was incorrectly referenced. The correct reference should read Post Office Protocol.

Trends

1. Several hackers/hacker groups appear to be using coordinated scans and probes from different sites.
2. Large numbers of scans and attacks continue to be directed at machines running the Linux operating system.
3. More phreaker tools are appearing on hacker Web sites.
4. Increase in organized crime using compromised Private Automatic Branch Exchanges (PABXs.)
5. Scanning for Internet Map Access Protocol (IMAP) and POP continues.
6. Significant increase in reports of NetBus and Back Orifice scanning.
7. Significant increase in the number of scans directed specifically against Domain Name Servers.

Viruses

A list of the top ten viruses infecting two or more sites as reported to various anti-virus vendors has been categorized into the two tables below. The first table list macro viruses, and the second table lists other viruses. Macro viruses have, historically, spread fastest due to their ability to be transferred by e-mail.

For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (i.e., boot, file, macro, multi-partite), trends (based on number of infections during the last three months reported), and approximate date first found.

Note: Virus reporting is normally 6 to 8 weeks behind the first discovery of infection. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages, as updates become available.

The viruses listed in the virus table have infected over 510 sites in December, which is a slight increase in the number of reported infections from the last prevalence table. The number 1 ranked virus for December/January accounted for 35 infected sites, and the last virus listed in the tables infected 17 sites. A total of 297 distinct viruses were reported this month, infecting over 2,000 sites.

Table 1 – Macro viruses:

Ranking	Common Virus Name	Type of Virus	Trends	Date
1	Concept	Macro	Steady	December 1996
2	CAP	Macro	Steady	April 1997
3	Class	Macro	Increasing	September 1998
4	Npad	Macro	Steady	December 1996
5	Wazzu	Macro	Steady	December 1996
6	Laroux	Macro	Steady	July 1997
7	MDMA	Macro	Steady	December 1996
8	ColdApe	Macro	NEW - No Trend	December 1998
9	Hark	Macro	NEW – No Trend	December 1998
10	Temple	Macro	NEW – No Trend	December 1998
Not Ranked	W2KM_PSD	Macro		January 1999

Table 2 – Other viruses:

Ranking	Common Virus Name	Type of Virus	Trends	Date
1	Form	Boot	Steady	September 1991
2	One_half	Multi	Decreasing	October 1995
3	Junkie	Multi	Steady	July 1994
4	AntiCMOS	Boot	Steady	October 1995
5	AntiEXE	Boot	Decreasing	September 1994
6	Empire.Monkey	Boot	Steady	July 1994
7	Parity_Boot	Boot	Steady	September 1993
8	Ripper	Boot	Steady	March 1994
9	Natas	Multi	Steady	October 1995
10	NYB	Boot	Decreasing	July 1994